DoD Cyberstrategy: Leveraging the Industrial Base

Office of the Deputy Assistant Secretary of Defense
for Industrial Policy

December 2010

Bottom Line Up Front

- “The risk of compromise in the [industrial base supply chain] is very real.”
- DoD’s cyber security strategy depends upon “… the U.S. commercial information technology sector remain[ing] the world's leader ….
- Requires “continuing investments in science, technology, and education at all levels.”

U.S. Cyber Strategy

Foreign Affairs, “Defending a New Domain,” William J. Lynn III, September/October 2010.

- Recognize cyberspace as a new domain of warfare.
- Active Defenses.
- Protect Critical Infrastructure.
- Cooperation.
- Leverage the U.S. technological base.

ICT Industrial Base Challenge
Reliable Supply

- Complexity of current hardware and software defies 100% testing
- Threats:
  - Counterfeiting
  - Tampering-damaging, or inserting mal-ware, into components
  - Anti-Tampering – reverse engineering of physical articles
- Trend to off-shoring manufacturing, development tools and manufacturing equipment is a risk to be managed

Information & Communications Technology (ICT) Industrial Base
Highly Simplified Supply Chain (HW/SW combined)

Weapon System
e.g. Vehicle

Sub System
e.g. Radio

Assembly/Component
e.g. microprocessor

Design and Manufacturing Tools

Large Integrator

Doing business with the government

Gov

Specialized Subcontractor

High reliability subsystems with domain knowledge

Defense, Aerospace, Automotive, Medical, Telecom, E-commerce, Oil Exploration

Component Manufacturer

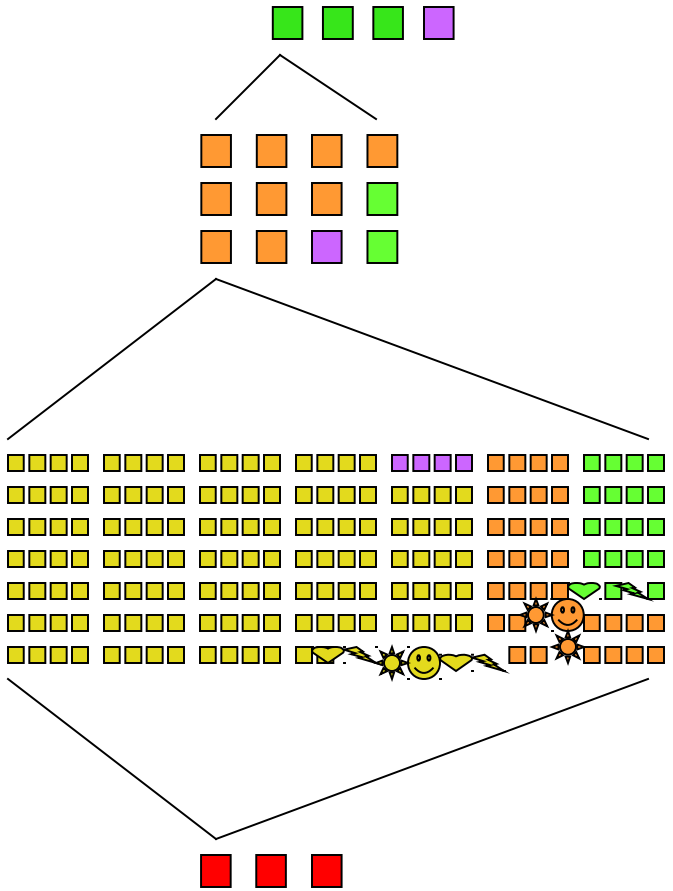
Piece Parts

Semiconductors, Software, Board Level Products, Connectors, Networking/Internet Products, Packaging, Security Products

Tooling Supplier

Design and Production Tools

HW Electronic Design Automation, SW Integrated Development Environment, CAD/CAE/CAM, PrCB and IC manufacturing equipment



ICT Industrial Base Supply Chain Dynamics

R&D Production Sustainment

Large Integrator
Doing business with the government

Gov

Meta-technology:
Technology Application
System of Systems

Civil Military
Role Reversal

Technology

Specialized Subcontractor

High reliability systems with domain knowledge
Automotive, Telecom, E-commerce, Medical, Aerospace, Defense

Components

Piece Parts

Board Level Products, Connectors, Networking/Internet Products, Packaging, Security Products, Semiconductors, Software

Tooling Supplier

Design and Production Tools

HW Electronic Design Automation, SW Integrated Development Environment, CAD/CAE/CAM, PCB and IC manufacturing equipment

Overseas

In the future world, it will still be possible to describe defense *applications* of technology, but increasingly meaningless to speak of defense *technology* as such: most technology used by defense will be drawn from the commercial sector."
Dr. Ashton Carter

e.g. Fewer military-specific hardware ASICs in favor of more software/firmware-driven applications on generic hardware

Leverage the U.S. commercial technological base

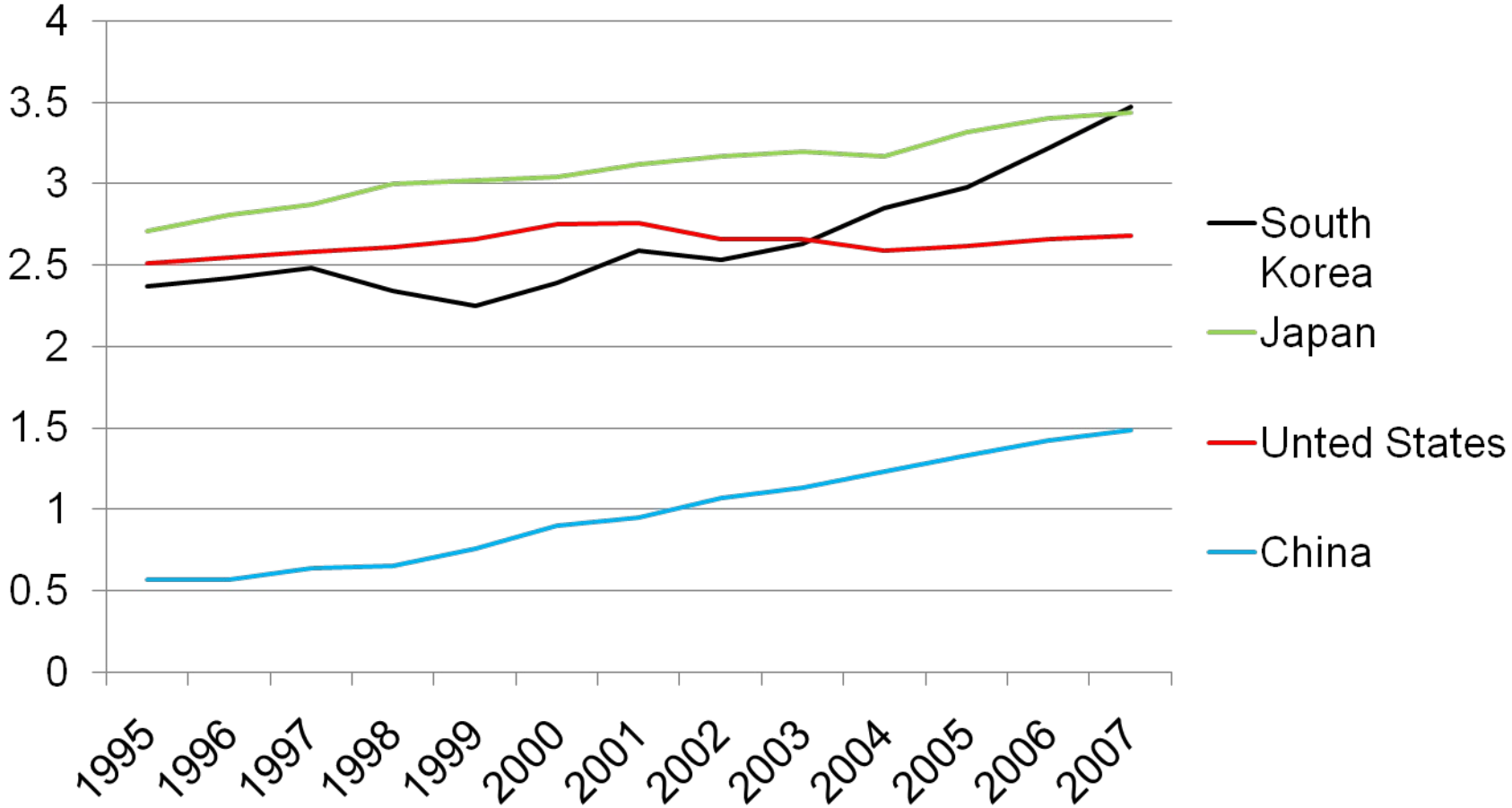
- Competitiveness: “Our economic security is part of our national security.”[1]
- What technologies does the U.S. want to be globally ubiquitous? Much easier to set the agenda if you’re #1 than #2.
- DoD is only 1% of the global demand for ICT – DoD R&D is never going to keep up with commercial R&D

[1] http://www.aia-aerospace.org/assets/speech_jones_06302010.pdf

Leverage the U.S. commercial technological base

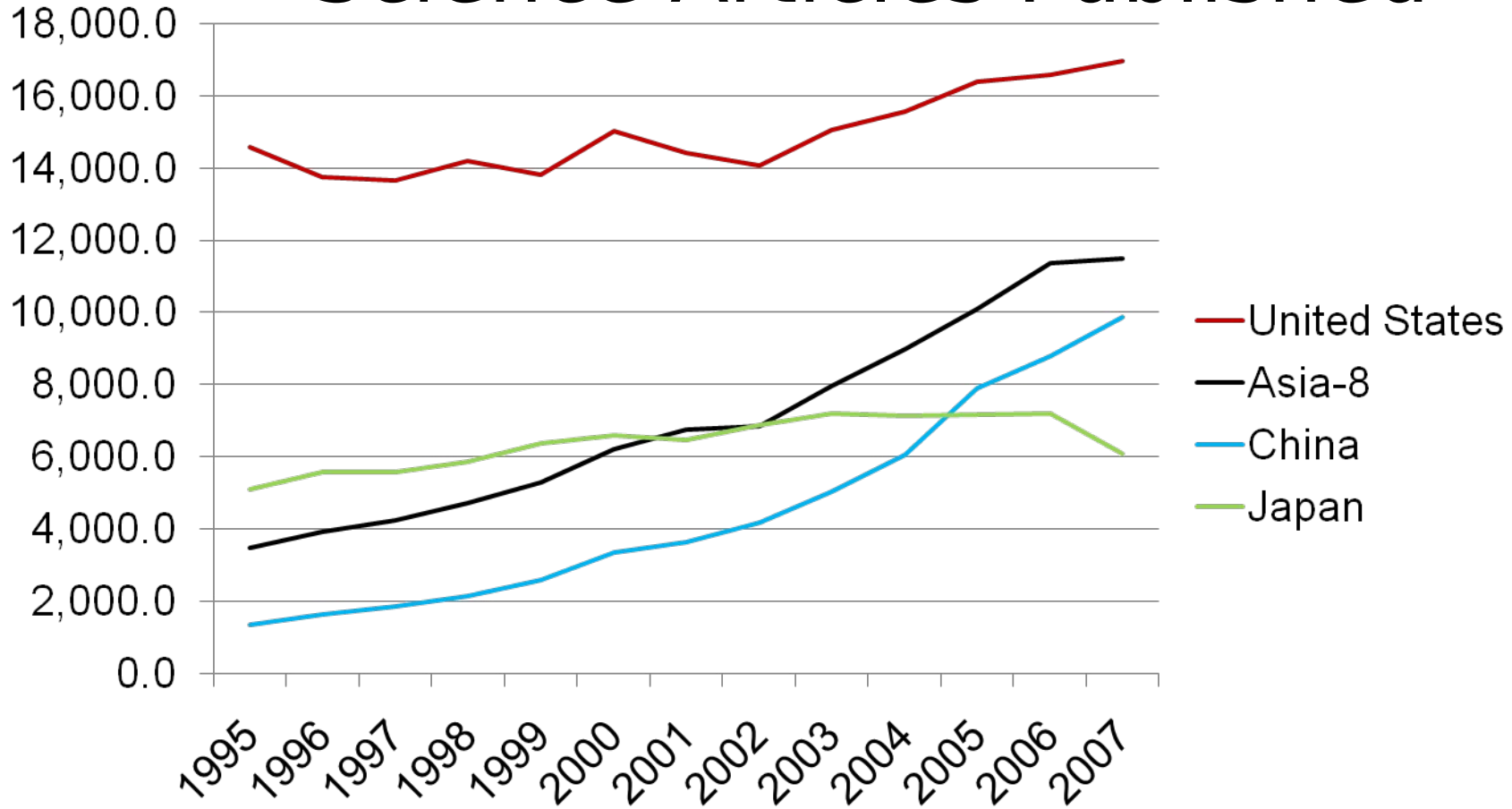
- Globalization is a fact of life
- Parsing, and then outsourcing, steps of the product development and manufacturing process is one of the drivers
- Another fact of life is that suppliers are not always content to remain at the bottom of the value chain: R&D follows manufacturing.
- …and manufacturing follows R&D.

Industrial Base
R&D as a Percent of GDP



2010 Science and Engineering Indicators, National Science Board, National Science Foundation.

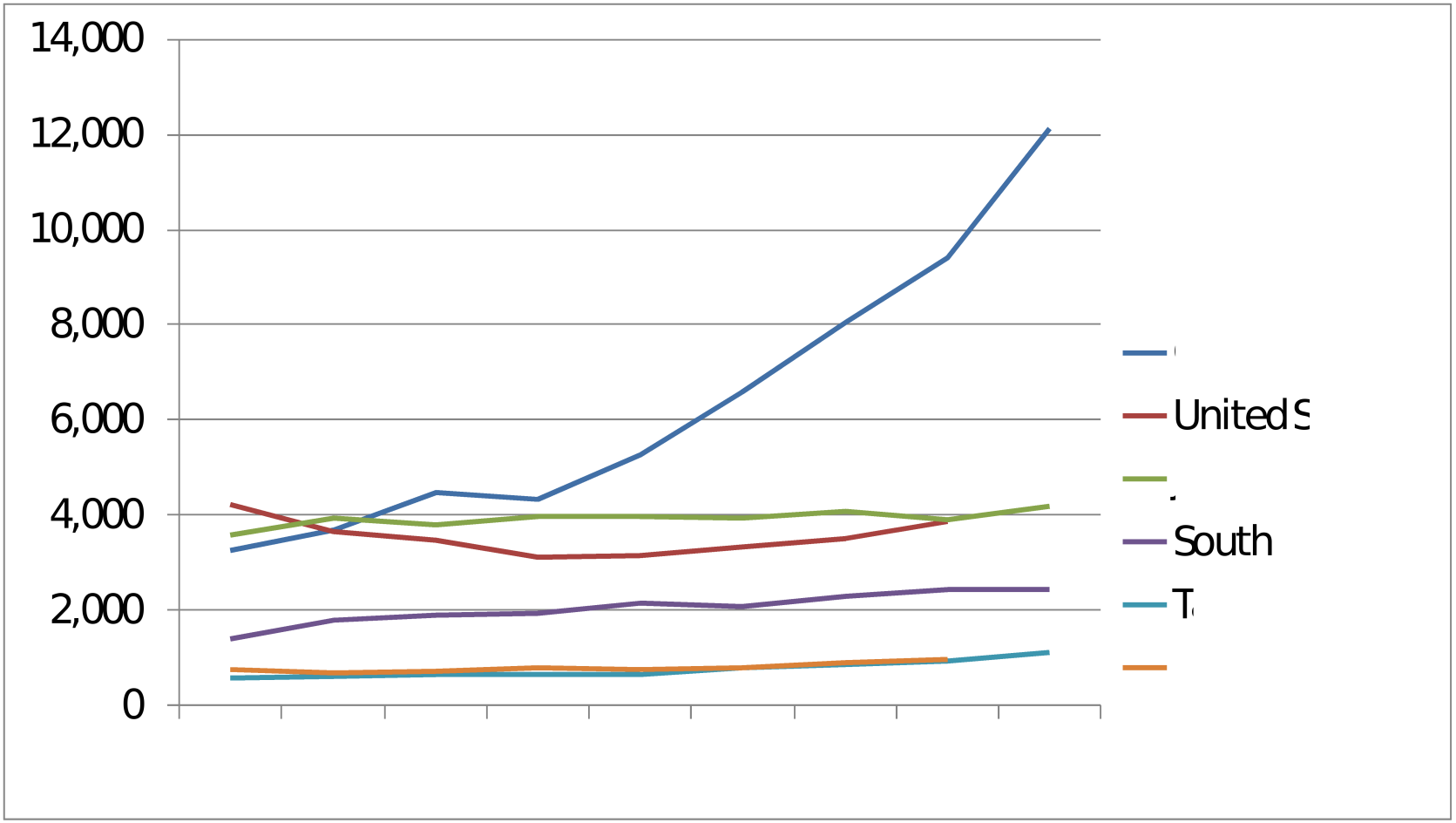
Human Capital: Engineering and Computer Science Articles Published



2010 Science and Engineering Indicators, National Science Board, National Science Foundation.

Human Capital:

PhD Degrees in Engineering, Math & Computer Science



2010 Science and Engineering Indicators, National Science Board, National Science Foundation.
* Excludes PhDs granted to foreign nationals at U.S. universities.

Leverage the U.S. commercial technological base: Plans and Actions

- Export Control Reform
  - Goal: Prevent harmful exports; facilitate useful ones. Higher fences around fewer things.

- Networking and Information Technology Research and Development (NITRD) Program coordinates the unclassified networking and information technology (IT) research and development (R&D) investments of fourteen Federal agencies.

- Section 931 Report to Congress: Implementation Strategy for Developing Leap-Ahead Cyber Operations Capabilities.

- Supply Chain Risk Management Directive Type Memorandum

- Program Protection Planning

Summary

- “The risk of compromise in the [industrial base supply chain] is very real.” It is complicated by foreign sources of supply.
- DoD’s cyber security strategy depends upon “…the U.S. commercial information technology sector remain[ing] the world's leader ….
- Requires “continuing investments in science, technology, and education at all levels.”
- DoD and the U.S. Government are:
  - investing in domestic R&D
  - initiating export control reform to remove barriers to international competition
  - taking steps to mitigate supply chain risk.

BACKUP

Background: Technology Fundamentals

- Software plays a huge role in modern electronics with a large portion of electronic hardware either being programmable or requiring software* instructions.
- Many features can be built with either hardware or software*.
- Trade space usually includes parameters like
  - Speed – high speed/real-time favors hardware like Application Specific Integrated Circuits (ASICs)
  - Power – low power consumption favors hardware
  - Quantity – high quantity makes hardware less expensive
  - Adaptability – favors software
  - Security
  - Standardization
- Embedded system: "special-purpose computer system designed to perform one or a few dedicated functions, often with real-time computing constraints. It is usually embedded as part of a complete device including hardware and mechanical parts." (Wikipedia)
- Business system: commodity computers with COTS operating systems and commercial-like applications.
- Increasingly embedded systems are connecting to outside networks blurring distinctions
- Obsolescence, tech refresh, incremental design - planning can be done up-front but it's a non-trivial program cost
- DoD ~1% of global IT market – pros and cons
- Logistics interoperability

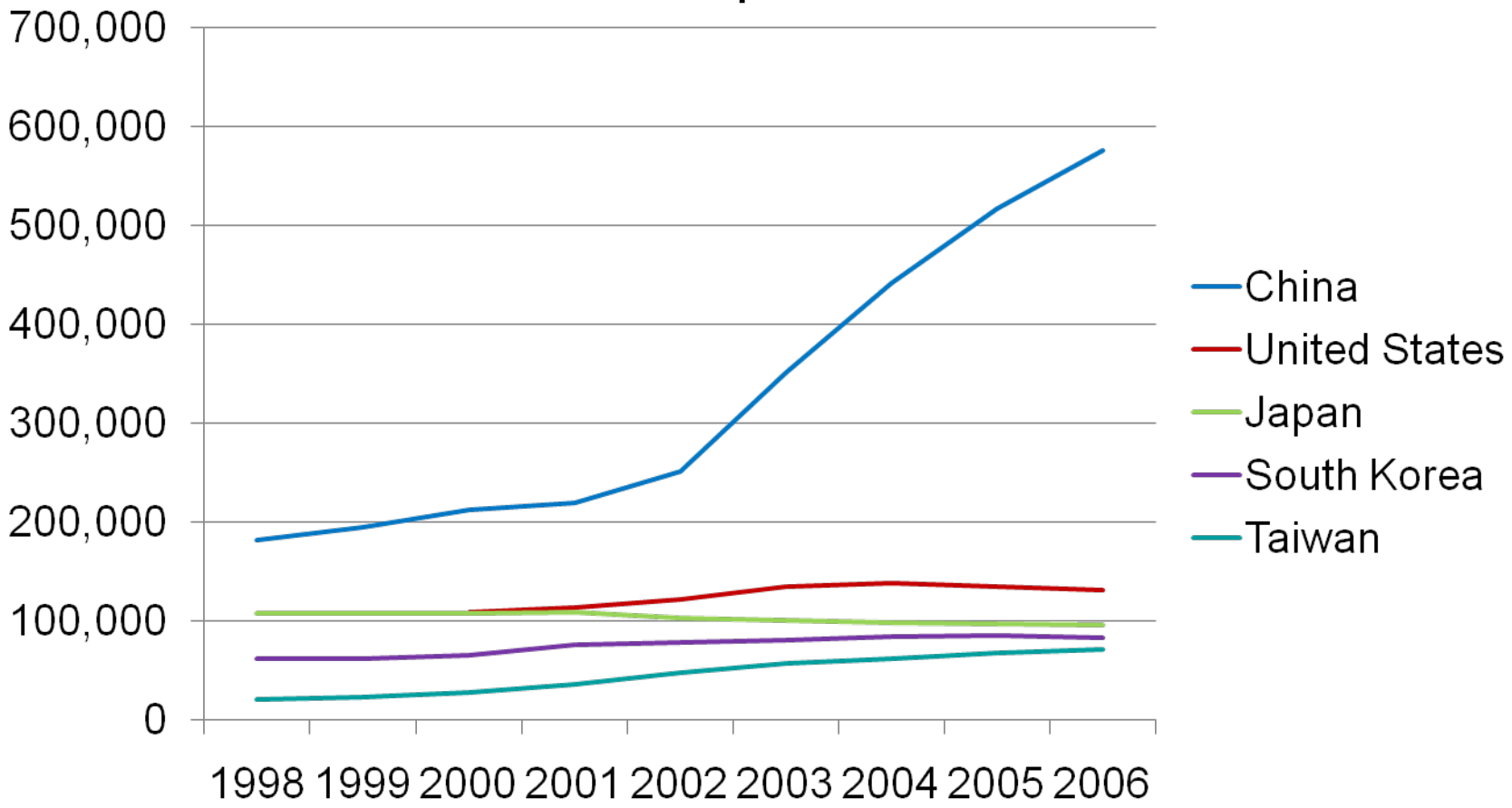
*Note: Firmware - a microprogram stored in ROM, designed to implement a function that had previously been provided in software.

Additional Pillar Elements

- IT acquisition reform
- Enduring Security Framework - public-private partnership with CEOs and CTOs
- Engineer way out of some problematic vulnerabilities
  - National Cyber Range program
  - fundamental research to improve ability to attribute attacks
  - rethink the Pentagon's network architecture with cybersecurity in mind

Human Capital:

Bachelor Degrees in Engineering, Math & Computer Science



2010 Science and Engineering Indicators, National Science Board, National Science Foundation.

Why some companies choose not to do business with the government

- FAR e.g. CAS
- ITAR
- DoD-specific benchmarks
- IP rights

Leverage the U.S. commercial technological base

- The NCO supports the NITRD Subcommittee, which coordinates the NITRD Program, and the organizations that report to the Subcommittee. The Subcommittee reports through the Committee on Technology to the Cabinet-level National Science and Technology Council. The organizations that report to the Subcommittee include two Interagency Working Groups (IWGs) and five Coordinating Groups (CGs) in the following R&D areas:
  - CSIA - Cyber Security and Information Assurance
  - HCI&IM - Human Computer Interaction and Information Management
  - HCSS - High Confidence Software and Systems
  - HEC - High End Computing
  - LSN - Large Scale Networking
  - SDP - Software Design and Productivity
  - SEW - Social, Economic, and Workforce Implications of IT and IT Workforce Development

  http://www.nitrd.gov

U.S. Cyber Strategy:
Leverage the U.S. technological base

- Human capital – strengthen cadre of cybersecurity professionals
  - Yet, long-term trends in human capital do not bode well. The United States has only 4.5 percent of the world's population. *The United States will lose its advantage in cyberspace if that advantage is predicated on simply amassing trained cybersecurity professionals.*
  - *over the next 20 years, many countries, including China and India, will train more highly proficient computer scientists than will the United States.*
- We must confront the cyber-defense challenge as we confront other military challenges: with a focus not on numbers but on *superior technology and productivity*.
- Such tools will be available only if the *U.S. commercial information technology sector* remains the world's leader -- something that will require *continuing investments in science, technology, and education at all levels*.
- Software and hardware are at risk of being tampered with even before they are linked together in an operational system. The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat.

Defense Industrial Base: Metatechnology

- In the future world, it will still be possible to describe defense *applications* of technology, but increasingly meaningless to speak of defense *technology* as such: most technology used by defense will be drawn from the commercial sector.”
- In the information technology community, the term technology development often refers to the development of new software or integration of both hardware and software systems, and has little to do with advances in science or engineering.”

ICT Industrial Base
Reasons to Manufacture Overseas
(ranking unknown)

- Cost of facility construction
- Operational costs
- Business tax structure
- ITAR
- Special subsidies
- Local market access
- Environmental Issues
- Offsets
- Oversight

Defense Industrial Base
Civil-Military Integration: Related Specialties

High Trust – damage limitations
- Financial (information assurance against advanced persistent threat, operational risk assessment)
- Gambling (threat assessment, behavior analysis, operational risk assessment)

High Reliability – design patterns
- Medical (6 9s “life critical”)
- Communications (5 9s “high availability”)
- Aerospace (“DO-178B (software) standard”)

Harsh Environments – physical reliability
- Aerospace (“DO-254 standard”)
- Oil/Gas Exploration (electronics packages embedded in drill bits “downhole”)
- Automotive (High Temps, high reliability, ISO/TS 16949)

Virtual Reality
- Entertainment (modeling and simulation)